1. Define benchmarking in a cybersecurity context.

In cyber security benchmarking means ability to benchmark your security architecture anonymously. The decision process involve having security products and services on board to make system more secure and stable. To benchmark the security architecture performing some analysis or reviewing the reviews of the peers, Performing gap analysis, Deciding and coming up with a strategic plan of having best suitable standards on the organizations would play a very important role.

2. List and explain the 3 suggestions provided by the author of the article.

* **Peer Pressure**
  + Peer knowledge could be a added advantage and would be helpful to know what security products and services needs to be implemented and how it is relatively good compared to the other peer companies with same domain.
* **Gap Analysis**
  + **Gap analysis would be a great way to analyses where company stands in specific areas of security and how it should improve the loop holes which it have.**
  + **There are different ways the gap analysis could be done**
    - Large security teams should analyses where I stands currently versus where it would have been according to the strategic plan
    - organization can have a gap analysis and recommendations from the third party to understand where the focus and efforts should be concentrated.
* **One-Person Show**
  + Typically in large organizations the security team will be huge and they also have more resources to concentrate on the gap analysis and other things to analyse where the company stand but in mid and small companies the team will be small and it has less people and also IT would be handling and will be held responsible and treated as a security team.